

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-134310

(43)Date of publication of application : 20.05.1997

(51)Int.Cl.

G06F 12/14
G06F 3/06

(21)Application number : 07-288930

(71)Applicant : FUJITSU LTD

(22)Date of filing : 07.11.1995

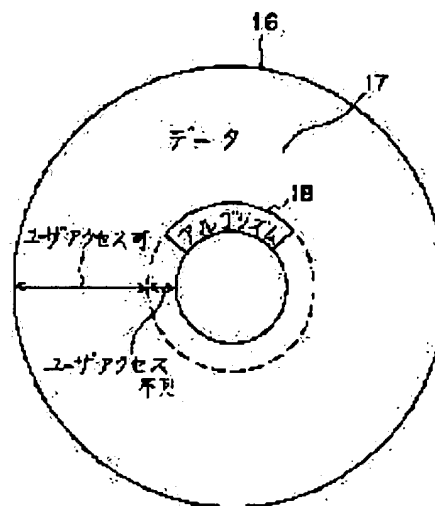
(72)Inventor : MASUDA TATSURO
KANEMOTO KOICHI
MURAKAMI KEIICHI
YOSHIOKA MAKOTO
KOTANI MASATAKE
YOSHIMOTO SHINICHI
FUJIWARA MASAO

(54) STORAGE MEDIUM AND METHOD FOR STORING DATA DECODING ALGORITHM

(57)Abstract:

PROBLEM TO BE SOLVED: To highly guarantee the security of ciphered data stored in a storage medium.

SOLUTION: Ciphered data 17 are stored in an area prepared in a storage medium 16 and allowed to be accessed by a user program and decoding algorithm for the data 17 is stored in an area not to be accessed by a user. A drive device loaded with the storage medium 16 extracts the algorithm 18 and decodes the data in accordance with the description of the algorithm 18. Since the data and its decoding algorithm are combined as a pair, a different ciphering method can be used in each data.



LEGAL STATUS

[Date of request for examination]

24.03.2000

[Date of sending the examiner's decision of rejection] 28.06.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-14331

[Date of requesting appeal against examiner's decision of rejection] 27.07.2005

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-134310

(43) 公開日 平成9年(1997)5月20日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		C 0 6 F 12/14	3 2 0 B
3/06	3 0 4		3/06	3 0 4 H

審査請求 未請求 請求項の数11 O L (全 6 頁)

(21) 出願番号 特願平7-288930

(22) 出願日 平成7年(1995)11月7日

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 増田 達朗
群馬県前橋市間屋町1丁目8番3号 株式会社富士通ターミナルシステムズ内

(72) 発明者 金元 浩一
群馬県前橋市間屋町1丁目8番3号 株式会社富士通ターミナルシステムズ内

(74) 代理人 弁理士 大曾 義之 (外1名)

最終頁に続く

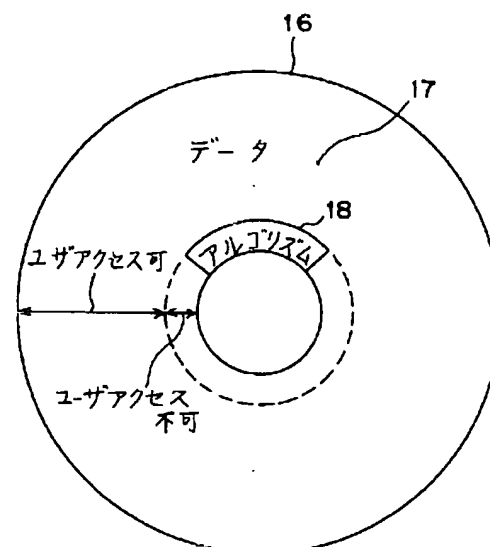
(54) 【発明の名称】 データの復号アルゴリズムを記憶する記憶媒体および方法

(57) 【要約】

【課題】 記憶媒体に格納された暗号化されたデータのセキュリティを高度に保証することを課題とする。

【解決手段】 記憶媒体16内のユーザプログラムによるアクセスが可能な領域にはデータ17が暗号化されて格納され、ユーザによるアクセスが不可能な領域にはデータ17の復号アルゴリズム18が格納される。記憶媒体16を装着されたドライブ装置はアルゴリズム18を取り出し、その記述にしたがってデータ17を復号する。データとその復号アルゴリズムがペアになっているので、データ毎に異なる暗号化方法を用いることができる。

媒体の記憶領域を示す図



【特許請求の範囲】

【請求項1】 暗号化されたデータを有するデータ領域手段と、

該データを復号するためのアルゴリズムを有するアルゴリズム領域手段とを備えることを特徴とする記憶媒体。

【請求項2】 前記データ領域手段は、前記記憶媒体中のユーザによるアクセスが可能な部分に設けられ、前記アルゴリズム領域手段は、該記憶媒体中のユーザによるアクセスが禁止された部分に設けられることを特徴とする請求項1記載の記憶媒体。

【請求項3】 データを有するデータ領域手段と、該データにアクセスするためのアルゴリズムを有するアルゴリズム領域手段とを備えることを特徴とする記憶媒体。

【請求項4】 前記データ領域手段は、前記記憶媒体中のユーザによるアクセスが可能な部分に設けられ、前記アルゴリズム領域手段は、該記憶媒体中のユーザによるアクセスが禁止された部分に設けられることを特徴とする請求項3記載の記憶媒体。

【請求項5】 暗号化されたデータと、該データを復号するためのアルゴリズムとを有する記憶媒体を装着する手段と、

前記記憶媒体から前記データとアルゴリズムを取り出し、該アルゴリズムに従って該データを復号する復号手段とを備えることを特徴とする復号装置。

【請求項6】 記憶媒体から取り出された、暗号化されたデータと該データを復号するためのアルゴリズムとを受け取る手段と、

前記アルゴリズムに従って前記データを復号する復号手段とを備えることを特徴とする復号装置。

【請求項7】 記憶媒体から取り出された、暗号化されたデータと該データを復号するための暗号化されたアルゴリズムとを受け取る手段と、

前記アルゴリズムの復号を外部装置に依頼し、復号されたアルゴリズムを受け取り、該復号されたアルゴリズムに従って前記データを復号する復号手段とを備えることを特徴とする復号装置。

【請求項8】 暗号化されたデータと該データを復号するためのアルゴリズムとをペアにして記憶することを特徴とする記憶方法。

【請求項9】 暗号化されたデータと該データにアクセスするためのアルゴリズムとをペアにして記憶することを特徴とする記憶方法。

【請求項10】 暗号化されたデータと、該データを復号するためのアルゴリズムとを有する記憶媒体から、該データとアルゴリズムを取り出し、

前記アルゴリズムに従って前記データを復号することを特徴とする復号方法。

【請求項11】 記憶媒体から取り出された、暗号化されたデータと該データを復号するためのアルゴリズムと

を受け取り、

前記アルゴリズムに従って前記データを復号することを特徴とする復号方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記録されたデータのセキュリティを保証する記憶媒体とその記憶方法、および暗号化されたデータの復号装置とその復号方法に関する。

【0002】

【従来の技術】情報処理技術の分野において、情報を記録する記憶媒体にはいくつかの種類のものがある。従来より用いられている記憶媒体としては、磁気テープ、磁気ディスク、光磁気ディスク、光ディスク等が知られており、今日ではますます多様化する傾向にある。このような記憶媒体に記録される情報には秘密性の高いものがあり、それらは暗号化されて記憶されることが多い。

【0003】例えば、磁気ディスク内の暗号化情報を復号する従来の情報処理システムでは、ドライブ装置に装着されたディスクから暗号化されたデータを読み出し、あらかじめ決められた復号アルゴリズムを用いてそれを復号している。復号アルゴリズムが与えられていない他のシステムではデータを解読することができず、ディスクのセキュリティが保証される。

【0004】

【発明が解決しようとする課題】しかしながら、上述のような従来のセキュリティ保証方法には次のような問題がある。

【0005】ディスク内のデータを復号するアルゴリズムがシステムで固有になっているため、一旦そのアルゴリズムが解読されると、他のシステムでも同じアルゴリズムを使用してデータを読むことができるようになる。

【0006】また、システムが保持する復号アルゴリズムに適応するような暗号化ディスクを作成するために、ディスク作成者にそのアルゴリズムを公開する必要がある。このため、第三者が公開されたアルゴリズムを手に入れて、暗号を解読する可能性がある。

【0007】このように復号アルゴリズムが単一であるため、それが何等かの方法で一旦破れると、暗号化されたデータのセキュリティが保証されないという問題がある。

【0008】本発明は、暗号化されたデータのセキュリティを高度に保証することのできる記憶媒体とその記憶方法を提供することを目的とする。

【0009】

【課題を解決するための手段】図1は、本発明の記憶媒体の原理図である。図1の記憶媒体1は、暗号化されたデータを有するデータ領域手段2と、そのデータを復号するためのアルゴリズムを有するアルゴリズム領域手段3とを備える。

【0010】データとその復号アルゴリズムがベアにして同一の媒体中に格納されるので、データ毎または媒体毎に異なる暗号化方法および復号方法を適用することが可能になる。このため、あるデータの復号アルゴリズムが第三者に知られた場合でも、それにより他のデータを復号することはできず、大多数のデータのセキュリティが守られることになる。

【0011】また、データ領域手段2は、記憶媒体1中のユーザによるアクセスが可能な部分に設けられ、アルゴリズム領域手段3は、記憶媒体1中のユーザによるアクセスが禁止された部分に設けられる。

【0012】このように、アルゴリズム領域手段3に対するユーザによるアクセスを禁止することで、その中に格納された復号アルゴリズムがユーザに知られる危険性を低くすることができる。この場合、データ領域手段2内のデータは簡単に取り出すことができるが、その暗号解読方法が取り出せないため、データのセキュリティが保証される。

【0013】また、データ領域手段2がデータを有し、アルゴリズム領域手段3がそのデータにアクセスするためのアルゴリズムを有するように構成することもできる。この場合も、データとそのアクセスアルゴリズムがベアにして同一の媒体中に格納され、データ毎または媒体毎に異なるアクセス方法を適用することが可能になる。したがって、データのセキュリティが高くなる。

【0014】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。図2は、本発明の記憶媒体を用いる第1の実施形態の情報処理システムの構成図である。図2の情報処理システムは、パーソナルコンピュータ（PC）11とドライブ装置12を備える。

【0015】ドライブ装置12は、復号部14とローダ15を有する復号機構13を備え、装着された媒体16から暗号化されたデータ17とその復号アルゴリズム18を読み出す。復号部14は、PC11から与えられたキーとローダ15から受け取ったアルゴリズム18を用いてデータ17を復号し、その結果をPC11に渡す。

【0016】復号機構13は、例えば、ドライブ装置12に備えられたマイクロ・プロセッサ等の処理装置により実現される。また、アルゴリズム18は、暗号解析方法や媒体16へのアクセス方法を含み、復号機構13が理解することのできる中間言語で記述されている。

【0017】図3は、媒体16の記憶領域の例を示している。図3の媒体16は、例えば、磁気ディスク、光ディスク、光磁気ディスク等であり、円形のディスク状の形をしている。ユーザによるアクセスが可能な領域にはデータ17が暗号化されて格納されており、ユーザによるアクセスが不可能な領域にはアルゴリズム18が格納されている。ここで、ユーザによるアクセスとは、ユーザのアプリケーション・プログラムがデバイスドライバ

等のソフトウェアを介して行うアクセスを意味する。ただし、ドライブ装置12はユーザアクセスが不可能な領域にもアクセスすることができる。

【0018】図4は、復号機構13によるデータの復号処理のフローチャートである。図4において処理が開始されると、復号機構13は、まずPC11からデータ17のリード要求とともに暗号解読用のキーを受け取る（ステップS1）。次に、ローダ15が媒体16中のアルゴリズム18をロードして復号部14に渡す（ステップS2）。

【0019】次に、復号部14が媒体16中のデータ17を読み出し（ステップS3）、アルゴリズム18に従い、キーを用いてデータ17を復号する（ステップS4）。このとき、例えば、アルゴリズム18に定められたデータ変換式中の変数にキーを代入して、データ17の変換を行う。そして、復号されたデータをPC11に渡して（ステップS5）、処理を終了する。

【0020】このように、アルゴリズム18はユーザからは参照することができず、ドライブ装置12の内部だけで使用されるので、アルゴリズム18自身の秘密性が高度に保持される。ユーザがアルゴリズム18を参照できないということは、暗号化されたデータ17のコピーを作ることではできても、媒体16のコピーは作れないことを意味する。したがって、データ17のセキュリティが保証される。

【0021】また、データ17とアルゴリズム18をベアにして媒体16に格納するので、データ毎にまたは媒体毎に異なる復号アルゴリズムを採用することができる。したがって、万が一アルゴリズムが漏れるようなことがあっても、それを用いて他の媒体のデータを解読することはできない。

【0022】第1の実施形態では、ドライブ装置12の内部でデータ17の復号を行っているが、これをその外部で行うことも可能である。図5は、データ17の復号をPC11内で行う第2の実施形態の情報処理システムの構成図である。図5において、基本的に図2と同様の構成要素には同じ符号が付けられている。

【0023】図5のPC11内では、アプリケーション・プログラム21が外部のドライブ装置12にアクセスする際に、アクセス専用のソフトウェアツールであるデバイスドライバ22を用いる。デバイスドライバ22は復号部23とローダ24を備え、図2の復号機構13と同様の役割を果たす。したがって、デバイスドライバ22によるデータ17の復号処理のフローは、基本的に図4と同様である。

【0024】ただし、この場合、復号部23は、ステップS1においてアプリケーション・プログラム21からリード要求とキーを受け取り、ステップS3においてドライブ装置12からデータ17を受け取り、ステップS5においてアプリケーション・プログラム21にデータ

を渡す。また、ローダ24は、ステップS2においてドライブ装置12からアルゴリズム18をロードする。

【0025】第2の実施形態においても、アルゴリズム18はアプリケーション・プログラム21から参照することができず、アルゴリズム18およびデータ17のセキュリティが保証される。

【0026】図6は、暗号化されたアルゴリズムを有する媒体を解読する第3の実施形態の情報処理システムの構成図である。図6において、基本的に図5と同様の構成要素には同じ符号が付けられている。

【0027】図6の情報処理システムは、通信ネットワーク32を介してPC11に結合した他の計算機であるサーバ33を備える。また、ドライブ装置12には、データ17とともに暗号化されたアルゴリズム34を格納する媒体35が装着される。デバイスドライバ22内のローダ31はアルゴリズム34をPC11内にロードした後、サーバ33にそれを送り、アルゴリズム34の復号を依頼する。そして、サーバ33が復号したアルゴリズムを受け取り、それを復号部23に渡す。復号部23は、渡されたアルゴリズムに従って、データ17を復号する。

【0028】図7は、図6のデバイスドライバ22によるデータの復号処理のフローチャートである。図7において処理が開始されると、デバイスドライバ22は、まずアプリケーション・プログラム21からデータ17のリード要求とともにデータ17の暗号解読用のキーを受け取る(ステップS11)。

【0029】次に、ローダ31がドライブ装置12から媒体35中のアルゴリズム34をロードする(ステップS12)。そして、ネットワーク32を介して、アルゴリズム34の復号をサーバ33に依頼し(ステップS13)、サーバ33から復号されたアルゴリズムを受け取って、復号部23に渡す(ステップS14)。

【0030】次に、復号部23が媒体35中のデータ17を読み出し(ステップS15)、復号されたアルゴリズムに従い、キーを用いてデータ17を復号する(ステップS16)。そして、復号されたデータをアプリケーション・プログラム21に渡して(ステップS17)、処理を終了する。

【0031】第3の実施形態によれば、復号アルゴリズム34そのものも暗号化されるので、媒体35のセキュリティはさらに高くなる。また、アルゴリズム34を解読するためのアルゴリズムはサーバ33に保持されているため、第3者は容易に知ることができない。

【0032】

【発明の効果】本発明によれば、暗号化されたデータとその復号アルゴリズムをペアにして記憶媒体に格納するため、データ毎にまたは媒体毎に異なる暗号化アルゴリズムを採用することができる。

【0033】また、ユーザは記憶媒体中の復号アルゴリズムにアクセスすることができないので、媒体全体をコピーすることができない。したがって、媒体中のデータのセキュリティが高くなる。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】第1の実施形態の構成図である。

【図3】媒体の記憶領域を示す図である。

【図4】復号機構の処理のフローチャートである。

【図5】第2の実施形態の構成図である。

【図6】第3の実施形態の構成図である。

【図7】デバイスドライバの処理のフローチャートである。

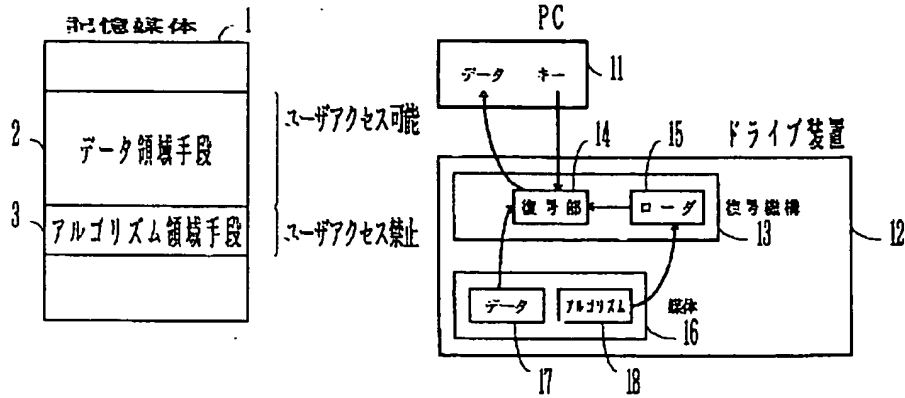
【符号の説明】

- 1、16、35 記憶媒体
- 2 データ領域手段
- 3 アルゴリズム領域手段
- 11 パーソナルコンピュータ
- 12 ドライブ装置
- 13 復号機構
- 14、23 復号部
- 15、24、31 ローダ
- 17 データ
- 18、34 アルゴリズム
- 21 アプリケーション・プログラム
- 22 デバイスドライバ
- 32 ネットワーク
- 33 サーバ

【図1】

【図2】

本発明の原理図第1の実施形態の構成図



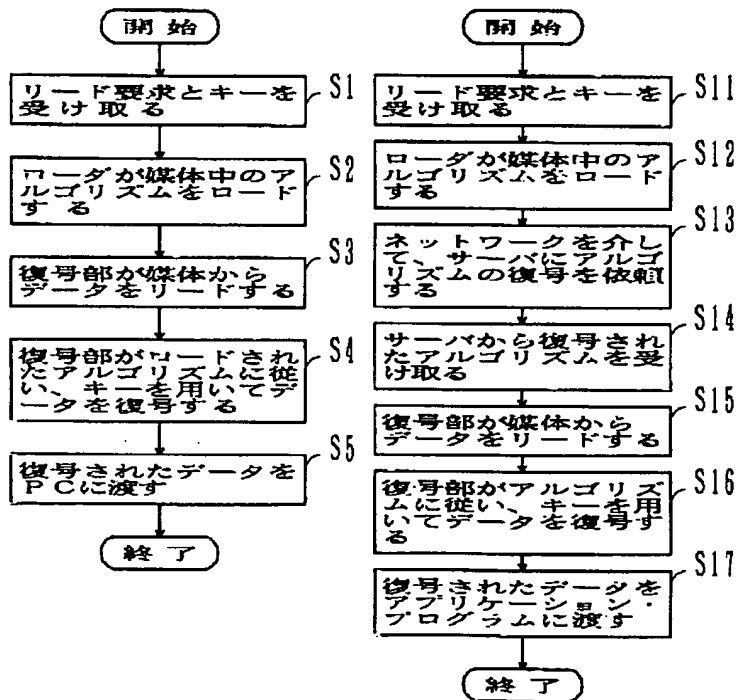
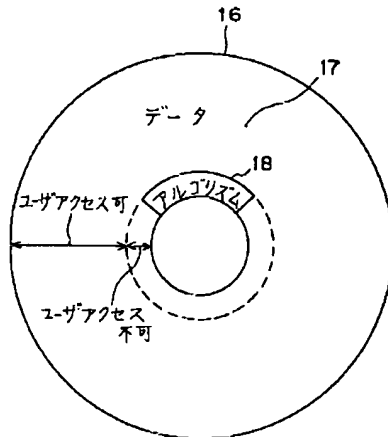
【図3】

媒体の記憶領域を示す図

【図4】

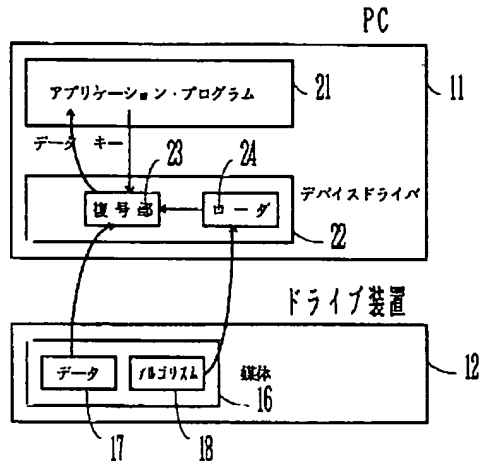
【図7】

復号機構の処理のフローチャート デバイスドライバの処理のフローチャート



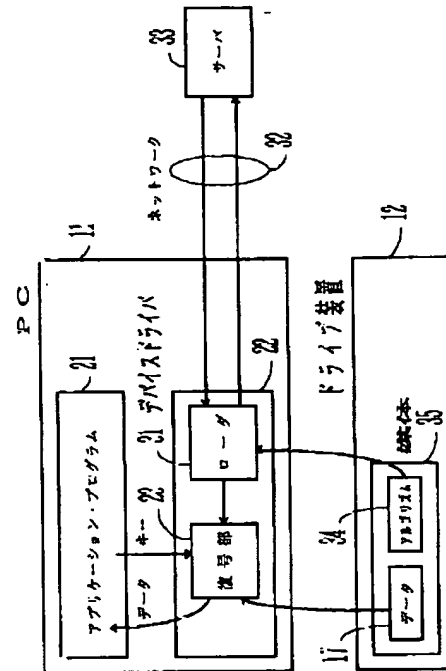
【図5】

第2の実施形態の構成図



【図6】

第3の実施形態の構成図



フロントページの続き

(72)発明者 村上 敬一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者 吉岡 誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者 小谷 誠剛
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者 吉本 真一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者 藤原 真雄
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内